УКРАЇНА

(19) UA (11) 86401 (13) C2

(51) МПК (2009)
G06F 7/58

МІНІСТЕРСТВО ОСВІТИ
І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ ДЕПАРТАМЕНТ
ІНТЕЛЕКТУАЛЬНОЇ
ВЛАСНОСТІ

ОПИС
ДО ПАТЕНТУ НА ВИНАХІД

(54) ГЕНЕРАТОР ПСЕВДОВИПАДКОВИХ ДВІЙКОВИХ ПОСЛІДОВНОСТЕЙ

(21) a200609286
(22) 23.08.2006
(24) 27.04.2009
(46) 27.04.2009, Бюл.№ 8, 2009 р.
(72) ОЛІЙНИК НАТАЛЯ ВОЛОДИМИРІВНА, UA, СОЛОЩУК МИХАЙЛО МИКОЛАЙОВИЧ, UA
(73) НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ "ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ", UA
(56) SU 1283950 A2, 15.01.1987
RU 2223593 C1, 10.02.2004
SU 1640699 A1, 07.04.1991
WO 2006024705 A1, 09.03.2006
US 5046036 A, 03.09.1991
RU 2081451 C1, 10.06.1997
UA 43182 C2, 15.11.2001
UA 72655 C2, 15.11.2004
GB 1404629 A, 03.09.1975
EP 1016959 A2, 05.07.2000
(57) Генератор псевдовипадкових двійкових послідовностей, який містить першу, другу та третю групи регістрів зсуву, з'єднаних з входами двовходових елементів "І", виходи яких з'єднані з відповідними входами суматорів по модулю два, які з'єднані з входами відповідних регістрів зсуву, генератор тактових імпульсів, з'єднаний із синхровходами регістрів зсуву, шину, з'єднану з блоком задання початкового стану, виходи якого з'єднані з елементами регістрів зсуву, двовходові елементи "І" групи з двовходових елементів, перші входи яких з'єднані з відповідними виходами регістрів зсуву, другі входи яких з'єднані з відповідними виходами першої групи виходів блока керування, друга група виходів якого з'єднана з відповідними першими виходами елементів "І", який **відрізняється** тим, що перша, друга та третя групи регістрів зсуву складаються відповідно з n-1, 1 та n-1 регістрів зсуву, nn двовходових елементів "І" об'єднані в n груп, виходи блока задання початкового стану з'єднані зі всіма елементами регістрів зсуву, при цьому елемент регістра зсуву складається з суматора по модулю два, до входів якого підключені виходи елемента "І" та D-тригера, до того ж елемент регістра зсуву має три входи, два з яких є входами елемента "І", а третій - входом D-тригера, та один вихід, що є виходом суматора по модулю два.

Винахід відноситься до галузі генерації випадкових чисел в обчислювальній техніці, техніці зв'язку і може бути використаний для захисту інформації обчислювальних систем, для статистичного аналізу випадкових процесів і полів.

Відомий генератор послідовностей випадкових чисел [патент РФ №2081451, МПК6 G06F7/58], що містить джерело шуму, генератор імпульсів, блок пам'яті, генератор напруги, що лінійно змінюється, схему порівняння, перший елемент "І-НІ", регістр зсуву, суматор по модулю два, елемент "НІ", другий елемент "І-НІ", перший і другий елементи "І".

Відомий генератор дозволяє одночасно формувати дві послідовності випадкових чисел.

Недоліком даного генератора є обмежена кількість послідовностей випадкових послідовностей, що генеруються, внаслідок того, що використання додаткової інверсної випадкової послідовності імпульсів дозволяє формувати одночасно з першою тільки одну іншу послідовність випадкових чисел.

Найбільш близьким по сукупності ознак є генератор псевдовипадкових двійкових послідовностей [А. с. СССР №1283950, МПК4 Н03К3/84], що містить n+m-1 регістрів зсуву, m n - входових суматорів по модулю два, n m -входових суматорів по модулю два, генератор тактових імпульсів, блок керування, m груп по n двовходових елементів "І", n груп по m двовходових елементів "І", групу з n·m двовходових елементів "І", блок за-

(19) UA (11) 86401 (13) C2

вдання початкового стану та шину "Установка". Виходи m n - входових та n m - входових суматорів по модулю два з'єднані з першими входами відповідних регістрів зсуву. Вихід генератора тактових імпульсів з'єднані з другими входами регістра зсуву. Перші входи двовходових елементів "І" групи з n·m двовходових елементів з'єднані з відповідними виходами регістрів зсуву. Другі входи двовходових елементів "І" групи з n·m двовходових елементів з'єднані з відповідними виходами першої групи виходів блока керування, друга група виходів якого з'єднана з відповідними першими виходами елементів "І" m груп по n двовходових елементів. Третя група виходів блока керування з'єднана з відповідними першими входами елементів "І" n груп по m двовходових елементів. Виходи відповідних розрядів регістрів зсуву з'єднані з відповідними другими входами елементів "І" груп по n та m двоходових елементів "І" відповідно, виходи елементів "І" яких з'єднані з відповідними m n - входових та n m - входових суматорів по модулю два.

Відомий генератор дозволяє одночасно генерувати псевдовипадкові числа різних числових послідовностей і матриць та керувати параметрами послідовностей, що генеруються.

Кількість різних числових послідовностей одного періоду, що генеруються відомим генератором, зумовлена обмеженою кількістю початкових станів, внаслідок завдання початкових станів тільки на елементах головної діагоналі матриці початкових станів.

В основу винаходу поставлена задача створення генератора псевдовипадкових послідовностей, у якому з'єднання блоку завдання початкового стану з кожним з елементів регістрів зсуву та нове конструктивне виконання регістру зсуву забезпечують збільшення кількості різних послідовностей одного періоду, що генеруються.

Поставлена задача вирішується тим, що в генераторі псевдовипадкових послідовностей, який містить першу, другу та третю групи регістрів зсуву, з'єднаних з входами двохвходових елементів "І", виходи яких з'єднані з відповідними входами суматорів по модулю два, які з'єднані з входами відповідних регістрів зсуву, генератор тактових імпульсів з'єднаний із синхровходами регістрів зсуву, шину "Установка", з'єднану з блоком завдання початкового стану, виходи якого з'єднані з елементами регістрів зсуву, двовходові елементи "І" групи з двовходових елементів, перші входи яких з'єднані з відповідними виходами регістрів зсуву, другі входи яких з'єднані з відповідними виходами першої групи виходів блока керування, друга група виходів якого з'єднана з відповідними першими виходами елементів "І", згідно винаходу, перша, друга та третя групи регістрів зсуву складаються з n-1, 1, n-1 регістрів зсуву відповідно, n двовходових елементів "І" об'єднані в n груп, виходи блоку завдання початкового стану з'єднані зі всіма елементами регістрів зсуву, при цьому елемент регістру зсуву складається з суматора по модулю два, до входів якого підключені виходи елемента "І" та D - тригера, до того ж елемент регістру зсуву має три входи, два з яких є входами елемента "І", а третій - входом D-тригера, та один вихід, що є виходом суматора по модулю два.

З'єднання у відомому генераторі блоку завдання початкового стану генератора псевдовипадкових послідовностей з кожним з елементів регістрів зсуву дозволяє завдавати початковий стан на всіх елементах матриці початкових станів.

З'єднання блоку керування з входами n груп по n двовходових елементів "І" забезпечує завдання значень коефіцієнтів. Виконання елементу регістру зсуву дозволяє реалізувати зсув елементів матриці, що приводить до збільшення кількості різних послідовностей одного періоду, що генеруються.

Суть винаходу пояснюється кресленнями, на яких подано:

Фіг.1 - схема генератора псевдовипадкових двійкових послідовностей;

Фіг.2 - схема регістру зсуву генератора псевдовипадкових послідовностей;

Фіг.3 - елемент регістра зсуву;

Фіг.4 - фрагмент регістру зсуву генератора псевдовипадкових двійкових послідовностей;

Фіг.5 - приклад виконання генератора псевдовипадкових двійкових послідовностей, де n=3;

Фіг.6 - часові діаграми роботи генератора псевдовипадкових двійкових послідовностей за Фіг.5.

Генератор псевдовипадкових двійкових послідовностей (Фіг.1) містить першу (I), другу (II) та третю (III) групи регістрів (1) зсуву по n-1, 1, n-1 регістрів зсуву відповідно, n груп (2) по n двовходових елементів "І", n·n - входових суматорів (3) по модулю два, генератор (4) тактових імпульсів, блок (5) керування, блок (6) завдання початкового стану, шину (7) "Установка" та групу (8) з n·n двовходових елементів "І".

Виходи регістрів 1 зсуву з'єднані з відповідними входами відповідних елементів "І" групи 2, крім того виходи першої групи регістрів 1 зсуву з'єднані з входами третьої групи регістрів 1 зсуву, виходи елементів "І" групи 2 з'єднані з відповідними входами суматорів 3 по модулю два, які з'єднані з входами відповідних регістрів 1 зсуву, вихід генератора 4 тактових імпульсів з'єднаний із синхровходами регістрів 1 зсуву, виходи блоку 6 завдання початкового стану з'єднані зі всіма елементами регістрів 1 зсуву, шина 7 "Установка" з'єднана з блоком 6 завдання початкового стану, виходи регістрів 1 зсуву з'єднані з групою. Перші входи двовходових елементів "І" групи 8 з n·n двовходових елементів з'єднані з відповідними виходами регістрів зсуву. Другі входи двовходових елементів "І" групи 8 з n·n двовходових елементів з'єднані з відповідними виходами першої групи виходів блока 5 керування, друга група виходів якого з'єднана з відповідними першими виходами елементів "І" n групи 2.

Вихід j-ого розряду i-ого регістра зсуву (j=1,2,…, i; i=1,2,...,n-1) першої групи i-розрядних регістрів зсуву (i=1,2,...,n-1) з'єднаний з j-им входом n груп по n двовходових елементів "І", вихід k-ого розряду n-ого регістра зсуву (k-1,2,...,n)

другої групи n - розрядних регістрів зсуву з'єднаний з k-им входом n груп 2 по n двовходових елементів "І", вихід q-ого розряду l-ого регістра зсуву (q=1,2,...,p; p=2n-l) третьої групи p - розрядних регістрів зсуву з'єднаний з q -им входом n груп 2 по n двовходових елементів "І", виходи n груп 2 по n двовходових елементів "І" з'єднані з відповідними входами відповідних n - входових суматорів 3 по модулю два.

Генератор містить у якості елемента регістра зсуву елемент (Фіг. 3), що має три входи, два з яких (1, 3) є входами елемента "І", а третій (2) - входом D-тригера, та один вихід суматора по модулю два, з'єднаних у такий спосіб, що виходи D-тригера та елемента "І" є входами суматора по модулю два:

Таким чином, регістр зсуву складається з послідовно з'єднаних елементів (Фіг.4), що являють собою діагоналі структурної матриці.

Генератор псевдовипадкових двійкових послідовностей працює таким чином.

За допомогою блока 6 завдається початковий стан кожного елемента регістрів зсуву. Потім за допомогою блоку 5 керування задаються значення коефіцієнтів, які надходять до відповідних входів n груп по n двовходових елементів 2 "І". Імпульси з тактового генератора 4 потрапляють на синхровходи регістрів 1 зсуву.

Генерація псевдовипадкових двійкових послідовностей відбувається у відповідності з матрицею $S[i+1] = A \cdot S[i] \cdot A^{-1}$, тобто

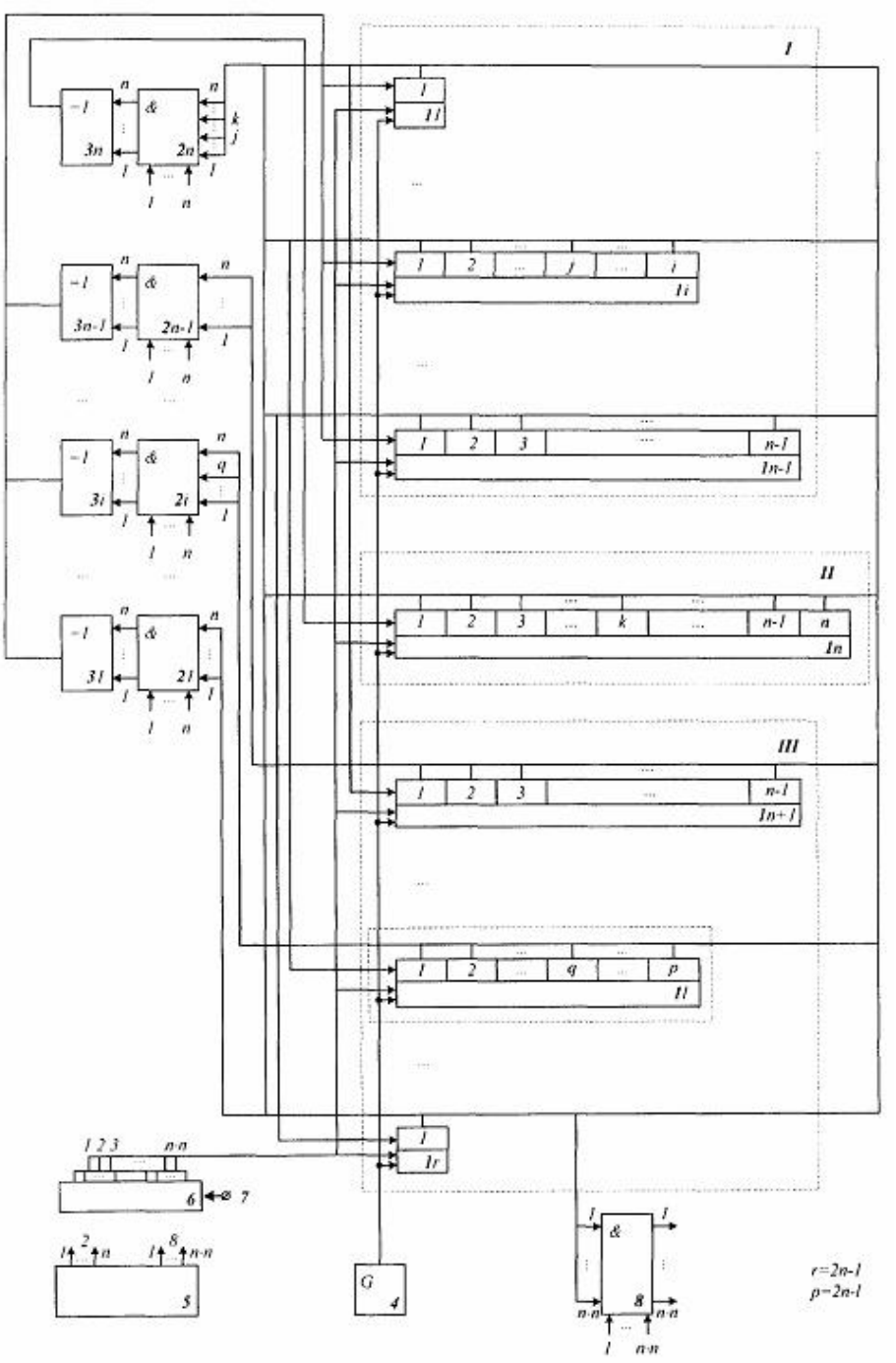
$$S[i+1] = \begin{bmatrix} a_{n-1} & a_{n-2} & a_{n-3} & \dots & a_1 & a_0 \\ 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & 1 & 0 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} S_{11}[i] & S_{12}[i] & S_{13}[i] & \dots & S_{1n}[i] \\ S_{21}[i] & S_{22}[i] & S_{23}[i] & \dots & S_{2n}[i] \\ S_{31}[i] & S_{32}[i] & S_{33}[i] & \dots & S_{3n}[i] \\ \dots & \dots & \dots & \dots & \dots \\ S_{n1}[i] & S_{n2}[i] & S_{n3}[i] & \dots & S_{nn}[i] \end{bmatrix} \cdot \begin{bmatrix} 0 & 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & \dots & 0 & 0 \\ 0 & 0 & 0 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 1 & a_{n-1} & a_{n-2} & \dots & a_2 & a_1 \end{bmatrix} =$$

$$= \begin{bmatrix} \sum_{k=1}^{n} a_{n-k} \cdot S_{kn} & \sum_{k=1}^{n} a_{n-k} \cdot S_{k1} + a_{n-1} \cdot \sum_{k=1}^{n} a_{n-k} \cdot S_{kn} & \sum_{k=1}^{n} a_{n-k} \cdot S_{k2} + a_{n-2} \cdot \sum_{k=1}^{n} a_{n-k} \cdot S_{kn} & \dots & \sum_{k=1}^{n} a_{n-k} \cdot S_{k,n-1} + a_1 \cdot \sum_{k=1}^{n} a_{n-k} \cdot S_{kn} \\ S_{1n} & S_{11} + a_{n-1} \cdot S_{1n} & S_{12} + a_{n-2} \cdot S_{1n} & \dots & S_{1,n-1} + a_1 \cdot S_{1n} \\ S_{2n} & S_{21} + a_{n-1} \cdot S_{2n} & S_{12} + a_{n-2} \cdot S_{1n} & \dots & S_{1,n-1} + a_1 \cdot S_{1n} \\ S_{3n} & S_{31} + a_{n-1} \cdot S_{3n} & S_{12} + a_{n-2} \cdot S_{1n} & \dots & S_{1,n-1} + a_1 \cdot S_{1n} \\ \dots & \dots & \dots & \dots & \dots \\ S_{nn} & S_{n-1,1} + a_{n-1} \cdot S_{n-1,n} & S_{n-1,2} + a_{n-2} \cdot S_{n-1,n} & \dots & S_{n-1,n-1} + a_1 \cdot S_{n-1,n} \end{bmatrix}$$

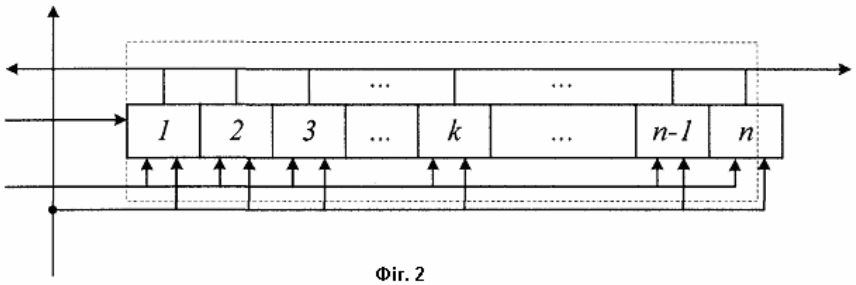
де матриця A - супровідна матриця, що містить у явному виді коефіцієнти свого характеристичного полінома $f(X)=X^n+a_{n-1}X^{n-1}+ \dots +a_1X+a_0$, матриця A^{-1} - матриця, зворотна матриці A; коефіцієнти $\{a_0, a_1, \dots, a_{n-1}\}$ яких задаються за допомогою блоку 5 керування, знак суми відповідає підсумовуванню по модулю два. Очевидно, що при переході від ;-ого стану генератора до (i+1)-стану інформація в матриці становища генератора S зсувається по діагоналях зверху вниз, а елементи першого рядка і першого стовпця обчислюються як лінійні комбінації деяких елементів матриці S, обумовлені структурою зворотного зв'язку генератора.

При кожному такті інформація в регістрах 1 зсувається на один розряд вправо, що відповідає зсуву інформації в матриці S на один розряд по діагоналі. У перші розряди всіх регістрів 1 зсуву записуються сигнали, значення яких обумовлюються в ланцюгах зворотного зв'язку n n - входових суматорів 3 по модулю два , n груп по n двовходових елементів 2 "І", що відповідає заповненню першого стовпця і першого рядка матриці S, причому послідовність станів будь-якого елемента матриці S генератора являє собою псевдовипадкову двійкову послідовність.

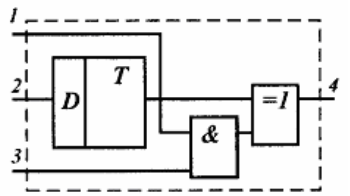
Таким чином, винахід що заявляється, дозволяє збільшити кількість різних послідовностей одного періоду, що генеруються.



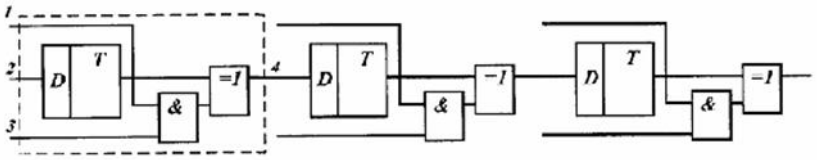
Фіг. 1



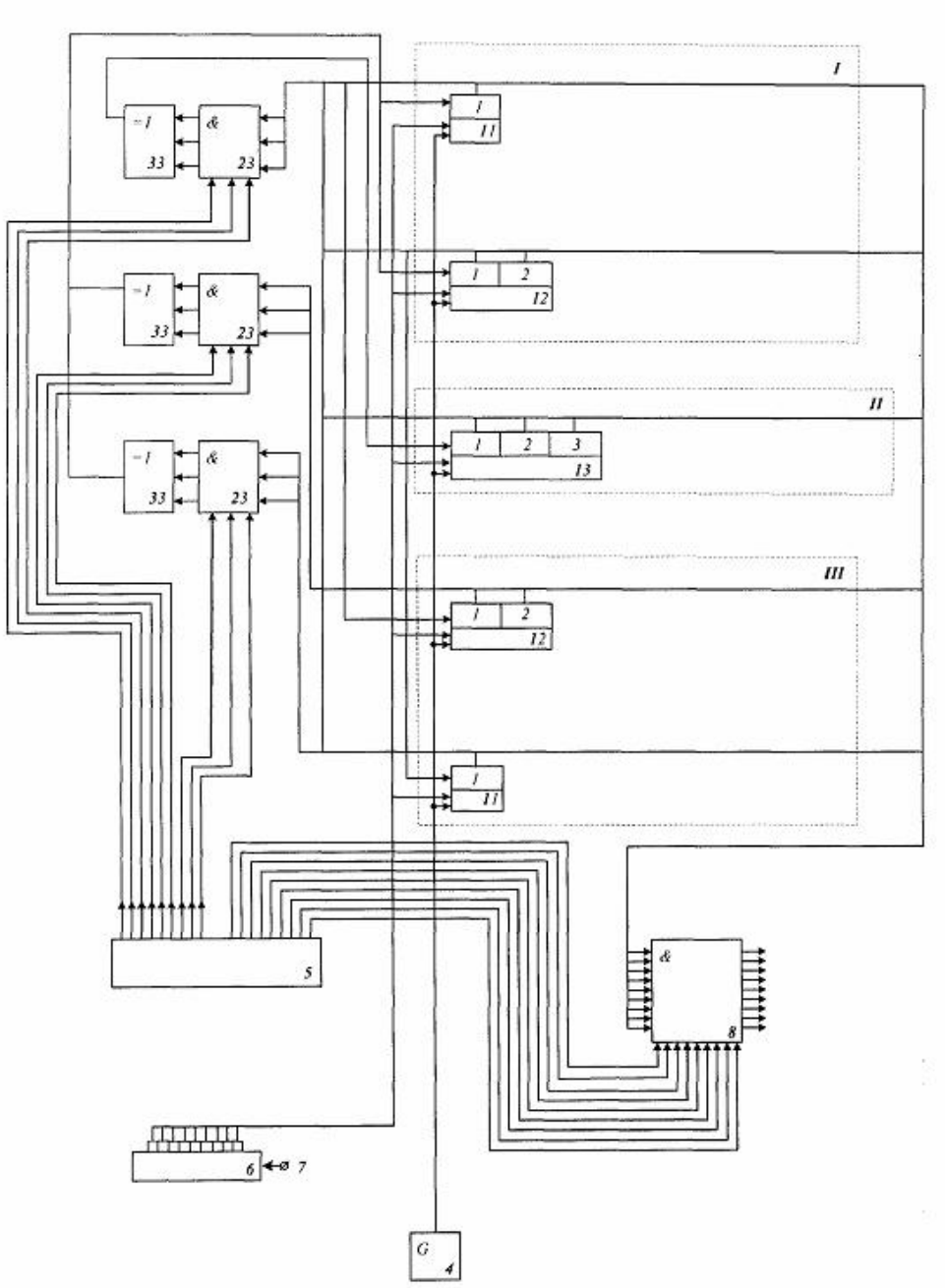
Фіг. 2



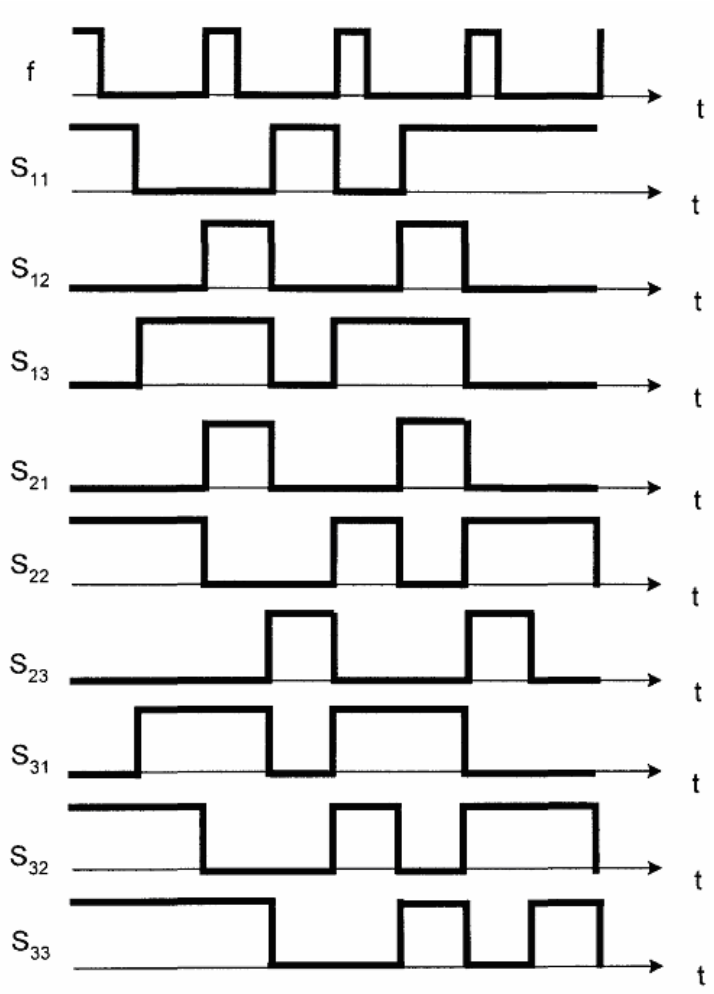
Фіг. 3



Фіг. 4



Фіг. 5



Фіг. 6

Комп'ютерна верстка Н. Лисенко Підписне Тираж 28 прим.

Міністерство освіти і науки України

Державний департамент інтелектуальної власності, вул. Урицького, 45, м. Київ, МСП, 03680, Україна

ДП "Український інститут промислової власності", вул. Глазунова, 1, м. Київ – 42, 01601